PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-200195
(43)Date of publication of application : 31.07.1997

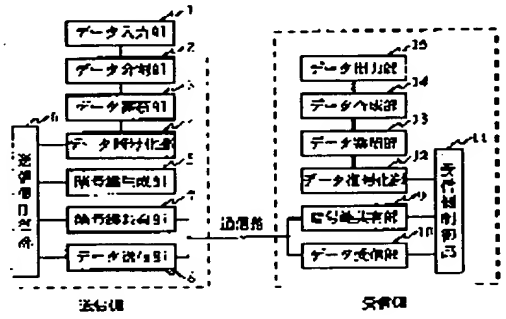
(51)Int.Cl. H04L 9/18
G09C 1/00
H04L 9/34

(21)Application number : 08-010104
(22)Date of filing : 24.01.1996

(71)Applicant : BROTHER IND LTD
(72)Inventor : NAKAMURA MICHIHIRO

(54) CIPHERING COMMUNICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To attain high speed transmission of ciphered data by using a ciphering key so as to apply decode processing to received ciphered data and synthesizing divided data in the order of numbers.
SOLUTION: A transmitter side informs ciphering communication to a receiver side, received transmission data are divided for 512-byte each by a data division section 2 and numbers 1-N are provided to the divided data in the division order and the resulting data are stored in a data storage section 3. The ciphered data are sent from a data transmission section 8 in order. The ciphered data are received by a data reception section 10 and decoded by a decoding section 12 by using a common shared ciphering key and stored in a data storage section 13. The stored data are synthesized in the order of division numbers for each page by a data synthesis section 14. The synthesized data are outputted by a data output section 15 and the entire transmission signal data are outputted finally.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

PAGE BLANK (USPTO)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－200195

(43)公開日　平成９年(1997)７月31日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/18			Ｈ０４Ｌ	9/00	６５１
Ｇ０９Ｃ	1/00	６１０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６１０Ｄ
Ｈ０４Ｌ	9/34			Ｈ０４Ｌ	9/00	６８１

審査請求　未請求　請求項の数３　ＯＬ　（全６頁）

(21)出願番号　特願平8－10104

(22)出願日　平成８年(1996)１月24日

(71)出願人　000005267
ブラザー工業株式会社
愛知県名古屋市瑞穂区苗代町15番１号

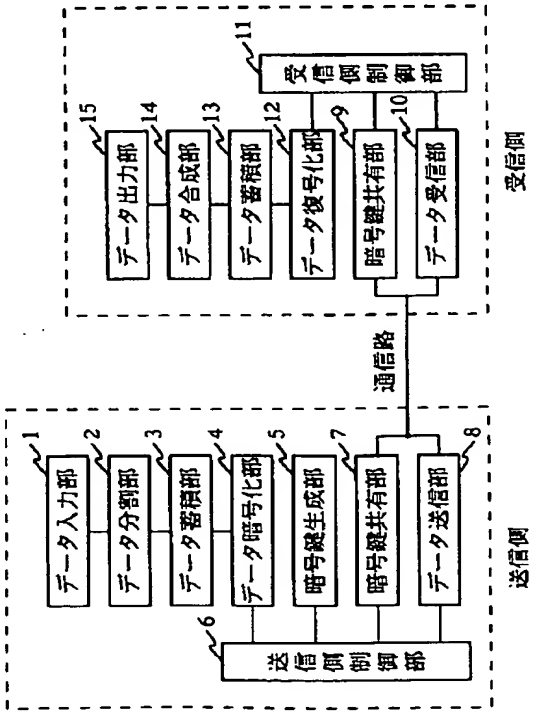
(72)発明者　中村　道弘
名古屋市瑞穂区苗代町15番１号ブラザー工業株式会社内

(54)【発明の名称】　暗号通信方式

(57)【要約】

【課題】　特に大きなデータを暗号化して送信する場合に、送信側と受信側とで高速に暗号化・復号化処理を行うことができ、また、暗号通信の機密性の強度を高めることができる暗号通信方式を提供することである。

【解決手段】　通信時に送信側と受信側とで送信データを暗号化するための暗号鍵を共有し、送信側では、送信データを特定の大きさに分割すると共に、順番に番号を付けて蓄積し、番号が付けられた分割データを暗号鍵を用いて暗号化処理して、受信側にデータの分割数の回数繰り返して送信し、受信側では、受信した暗号化データを暗号鍵を用いて復号処理し、復号された各分割データをデータに付けられた番号順に合成することによって元の送信データに復元する。



1

【特許請求の範囲】

【請求項１】　データを送信側で暗号化して受信側に送信する暗号通信方式において、

前記送信側では、送信データを特定の大きさに分割して、その分割されたデータに順番に番号を付けて蓄積する一方、前記番号が付けられた分割データをそれぞれ暗号鍵を用いて暗号化処理した後、その各暗号化データを前記分割回数分繰り返して受信側に送信し、

前記受信側では、受信した前記各暗号化データを前記受信側と共有する前記暗号鍵を用いて復号処理し、その復号された各分割データを前記番号の順番に従って合成することを特徴とする暗号通信方式。

【請求項２】　データを送信側で暗号化して受信側に送信する暗号通信方式において、

前記送信側では、送信データを特定の大きさに分割して、その分割されたデータに順番に番号を付けて蓄積する一方、前記分割数と同数の互いに異なる暗号鍵を生成して、それ等の暗号鍵と前記各分割データの番号とを１対１に対応させると共に、前記各分割データをそれぞれ対応する前記暗号鍵を用いて暗号化処理した後、その各暗号化データを前記分割回数分繰り返して受信側に送信し、

前記受信側では、受信した前記各暗号化データを前記受信側と共有する前記各暗号鍵を用いて復号処理し、その復号された各分割データを前記番号の順番に従って合成することを特徴とする暗号通信方式。

【請求項３】　データを送信側で暗号化して受信側に送信する暗号通信方式において、

前記送信側では、送信データをｎバイト単位でＮ行×Ｍ列に分割して、その各列毎に列方向のデータを合成することにより、Ｎ×ｎバイトのデータを作成して、各列のデータ毎にｉ（１≦ｉ≦Ｍ）の番号を付けて蓄積する一方、そのＭ列と同数の互いに異なる暗号鍵を生成して、それ等の暗号鍵と前記各分割データの番号とを１対１に対応させると共に、前記各分割データをそれぞれ対応する前記暗号鍵を用いて暗号化処理した後、その各暗号化データを前記Ｍ回分繰り返して受信側に送信し、

前記受信側では、受信した前記各暗号化データを前記受信側と共有する前記各暗号鍵を用いて復号処理し、その復号された各分割データを前記Ｎ行×Ｍ列に合成することを特徴とする暗号通信方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データを送信側で暗号化して受信側に送信する暗号通信方式に関するものである。

【０００２】

【従来の技術】従来、この種の暗号通信方式においては、データを送信側から受信側に送信する場合、その送信データのデータ全体を送信側で一つの暗号鍵により暗

2

号化処理した後に受信側に送信されていた。

【０００３】

【発明が解決しようとする課題】しかしながら、従来の暗号通信方式によれば、データ全体を一度に暗号化処理して送信を行うので、特に、容量の大きなデータを送信する場合には、暗号化処理に非常に時間を要し、送信を開始するまでに非常に時間がかかると共に、受信側においても、受信した暗号化データの復号に非常に大きな時間を要する問題点があった。

【０００４】また、データ全体を一つの暗号鍵で暗号化処理を行っていたために、その暗号鍵が知られてしまうと、暗号化データ全体の内容が知られてしまうという問題点があった。

【０００５】本発明は、上述した問題点を解決するためになされたものであり、データを分割した分割データを順次暗号化処理して送信することにより、高速に暗号化データの送信を行うことができる暗号通信方式を提供することである。

【０００６】

【課題を解決するための手段】この目的を達成するために、本発明の請求項１に記載の暗号通信方式は、データを送信側で暗号化して受信側に送信する方式を対象として、特に、前記送信側では、送信データを特定の大きさに分割して、その分割されたデータに順番に番号を付けて蓄積する一方、前記番号が付けられた分割データをそれぞれ暗号鍵を用いて暗号化処理した後、その各暗号化データを前記分割回数分繰り返して受信側に送信し、前記受信側では、受信した前記各暗号化データを前記受信側と共有する前記暗号鍵を用いて復号処理し、その復号された各分割データを前記番号の順番に従って合成するようにしている。従って、データを分割した分割データを順次暗号化処理して送信することにより、高速に暗号化データの送信を行うことができる。

【０００７】また、請求項２に記載の暗号通信方式は、データを送信側で暗号化して受信側に送信する方式を対象として、特に、前記送信側では、送信データを特定の大きさに分割して、その分割されたデータに順番に番号を付けて蓄積する一方、前記分割数と同数の互いに異なる暗号鍵を生成して、それ等の暗号鍵と前記各分割データの番号とを１対１に対応させると共に、前記各分割データをそれぞれ対応する前記暗号鍵を用いて暗号化処理した後、その各暗号化データを前記分割回数分繰り返して受信側に送信し、前記受信側では、受信した前記各暗号化データを前記受信側と共有する前記各暗号鍵を用いて復号処理し、その復号された各分割データを前記番号の順番に従って合成するようにしている。従って、分割した分割データをそれぞれ異なる暗号鍵で暗号化することにより、データの機密性の高い暗号通信を行うことができる。

【０００８】さらに、請求項３に記載の暗号通信方式

は、データを送信側で暗号化して受信側に送信する方式を対象として、特に、前記送信側では、送信データをｎバイト単位でＮ行×Ｍ列に分割して、その各列毎に列方向のデータを合成することにより、Ｎ×ｎバイトのデータを作成して、各列のデータ毎にｉ（１≦ｉ≦Ｍ）の番号を付けて蓄積する一方、そのＭ列と同数の互いに異なる暗号鍵を生成して、それ等の暗号鍵と前記各分割データの番号とを１対１に対応させると共に、前記各分割データをそれぞれ対応する前記暗号鍵を用いて暗号化処理した後、その各暗号化データを前記Ｍ回分繰り返して受信側に送信し、前記受信側では、受信した前記各暗号化データを前記受信側と共有する前記各暗号鍵を用いて復号処理し、その復号された各分割データを前記Ｎ行×Ｍ列に合成するようにしている。従って、分割した分割データをそれぞれ異なる暗号鍵で暗号化することにより、データの機密性の高い暗号通信を行うことができる。

【０００９】

【発明の実施の形態】以下に、本発明の暗号通信方式を具体化した実施の形態について図面を参照して説明する。

【００１０】図１は本実施の形態における暗号通信方式の構成を示すブロック図である。

【００１１】データを送信する送信側は、データ入力部１、データ分割部２、データ蓄積部３、データ暗号化部４、暗号鍵生成部５、送信側制御部６、暗号鍵共有部７、データ送信部８等から構成されている。

【００１２】前記データ入力部１は、入力装置（例えば、ファクシミリ装置の読取装置及びコンピュータ等）からのデータを入力するものである。前記データ分割部２は、入力されたデータを５１２バイト毎のデータに分割するものであり、分割データの最後のものには、ちょうど５１２バイトになるように付加データとして、アスキーコードの“空白”文字を表わす“０ｘ２０”（１６進数）を追加して５１２バイトにする操作をするようにしている。前記データ蓄積部３は、データ分割部２で分割された分割データに分割された順番に分割番号を付けて蓄積するものである。前記データ暗号化部４は、分割番号が付けられた分割データを暗号鍵を用いて暗号化処理するものであり、分割データは分割番号と一緒に暗号化されるものである。前記暗号鍵生成部５は、暗号化処理を行うための暗号鍵を生成するためのものであって、暗号通信を行う度にランダムな暗号鍵を生成するようになっている。

【００１３】また、前記送信側制御部６は、送信側の制御処理全体を実行するものであり、データ暗号化処理の制御、暗号鍵生成処理の制御、受信側との暗号鍵共有処理の制御、データ送信処理の制御、通信手順における諸々の制御を実行するものである。前記暗号鍵共有部７は、暗号鍵生成部５で生成された暗号鍵を受信側とで共有するための処理を行うものであり、公開鍵暗号方式を用いて暗号鍵の共有を行うものである。前記データ送信部８は、データを受信側に送信する処理を行うものである。

【００１４】一方、本実施の形態の受信側は、暗号鍵共有部９、データ受信部１０、受信側制御部１１、データ復号化部１２、データ蓄積部１３、データ合成部１４、データ出力部１５等から構成される。

【００１５】前記暗号鍵共有部９は、送信側で生成された暗号鍵を通信の際に共有するための処理を行うものである。前記データ受信部１０は、送信側から送信されたデータを受信する処理を行うものである。前記受信側制御部１１は、受信側の制御処理全体を実行するものであり、送信側との暗号鍵共有処理の制御、データ受信処理の制御、受信データの復号化処理の制御、復号データの合成処理の制御、通信手順における諸々の制御を実行するものである。前記データ復号化部１２は、受信データを前記暗号鍵を用いて復号処理するものであり、分割データの個数回復号処理を行うものである。前記データ蓄積部１３は、復号処理されたデータを蓄積するためのものである。前記データ合成部１４は、復号データを分割番号の順番に合成するためのものである。前記データ出力部１５は、前記データ合成部１４で合成されたデータを、受信側装置の出力装置に出力するものである。

【００１６】図２は本実施の形態における暗号通信方式の送信処理手順を示すフローチャートである。

【００１７】先ず、送信側では、コンピュータで作成された送信データがデータ入力部１により入力され（Ｓ１、Ｓはステップを示す。以下同様）、送信者によって暗号通信が選択されれば（Ｓ２：Ｙ）、暗号送信手順を行い、暗号通信が選択されなければ（Ｓ２：Ｎ）、通常の暗号を利用しない通信が行われる。暗号通信の場合には（Ｓ２：Ｙ）、受信側との通信接続の際に、暗号通信の通知が受信側に通知される（Ｓ３）。入力された送信データは、５１２バイト毎にデータ分割部２で分割される（Ｓ４）。この時、分割されたデータの最後の分割データがちょうど５１２バイトになるように最終分割データは調節される。ここで、Ｎ個に分割されたデータは、分割された順番に１～Ｎの番号が付けられ、図４に示されるようなフォーマットで分割番号が分割データに追加されて、データ蓄積部３に蓄積される（Ｓ５）。

【００１８】データの暗号化処理に使用される暗号鍵は暗号鍵生成部５で作成され（Ｓ６）、暗号鍵共有部７で公開鍵暗号方式を用いて受信側に送信され、受信側と暗号鍵の共有を行う（Ｓ７）。この暗号鍵の共有が完了すると、データ暗号化部４において分割番号を含めた分割データを暗号鍵を用いて暗号化処理し（Ｓ８）、暗号化された暗号化データを順番にデータ送信部８から送信する（Ｓ９）。この時、暗号化処理と暗号化データの送信は同時に動作する処理であり、ｎ個目の分割データが暗号化処理されている時には、ｎ－１個目の暗号化データ

が送信される。暗化号データの送信が完了すると、終了メッセージを送信して通信を終了する（Ｓ１０）。

【００１９】図３は本実施の形態における暗号通信方式の受信処理手順を示すフローチャートである。

【００２０】通信接続の際に暗号通信が通知されると（Ｓ２１：Ｙ）、受信側の暗号鍵が暗号鍵共有部９で共有され（Ｓ２２）、暗号化データの受信準備が完了する。

【００２１】暗号化データは、データ受信部１０によって受信されると共に（Ｓ２３）、共有された暗号鍵を用いてデータ復号化部１２によって復号処理され（Ｓ２４）、データ蓄積部１３に蓄積される。蓄積されたデータは、図４に示すフォーマットであるので、データ合成部１４によって分割番号の順番にページ単位毎に合成される（Ｓ２５）。合成されたデータはデータ出力部１５によって出力され（Ｓ２６）、最終的に送信データ全体を出力することができる。通信終了メッセージを受信すると、通信を終了する（Ｓ２７）。

【００２２】このように、送信データに比べて分割データは小さいので、暗号化処理は短い時間で完了して送信されるので送信開始までの時間を短くすることができ、数ページに亙る文章等の場合には、順次暗号データの復号処理を行うことができ、ページ単位毎に合成を行って出力するので、送信データ全体を一度に暗号化処理するよりも高速に暗号データの送信・出力を行うことができる。

【００２３】また、前記実施の形態では、データの分割サイズは５１２バイトであるが、他の分割サイズでも可能であり、最後の分割データのサイズ調整のためにアスキーコードの“０ｘ２０”を使用しているが、“０ｘ００”等の他のコードでも可能である。また、復号データの合成はページ単位で行っているが、復号されたデータを合成せずに順次出力することも可能である。

【００２４】また、前記実施の形態では、コンピュータによる暗号通信の場合について述べたが、ファクシミリ通信にこの暗号通信方式を使用することももちろん可能である。

【００２５】また、分割データをそれぞれ異なる暗号鍵を用いて暗号化処理を行い、暗号化データとすることも可能である。

【００２６】次に、本発明を具体化した他の実施の形態の暗号通信方式について図２及び図３を参照して説明する。

【００２７】先ず、送信側では、コンピュータで作成された送信データがデータ入力部１により入力され（Ｓ１）、送信者によって暗号通信が選択されれば（Ｓ２：Ｙ）、暗号送信手順を行い、暗号通信が選択されなければ（Ｓ２：Ｎ）、通常の暗号を利用しない通信が行われる。暗号通信の場合には（Ｓ２：Ｙ）、受信側との通信接続の際に、暗号通信の通知が受信側に通知される（Ｓ３）。入力された送信データを４０９６バイトと仮定し、行列を１バイト単位として、Ｎ＝６４、Ｍ＝６４とすると、送信データは図５のように示される。この送信データは、データ分割部２において分割処理され（Ｓ４）、１列目のデータは、

Ｄ１＝Ｍ１Ｎ１，Ｍ１Ｎ２，Ｍ１Ｎ３，．．．，Ｍ１Ｎ６４

となる。

【００２８】以下送信データは、順次６４列目のデータまで同様に分割される。

【００２９】Ｄ６４＝Ｍ６４Ｎ１，Ｍ６４Ｎ２，Ｍ６４Ｎ３，．．．，Ｍ６４Ｎ６４

ここで、これらの６４個に分割されたデータは、分割された順番に１～６４の分割番号が付けられ、図６のようなフォーマットで分割データに追加されて、データ蓄積部３に蓄積される（Ｓ５）。

【００３０】データの暗号化処理に使用される暗号鍵は、Ｍ＝６４個分だけ暗号鍵生成部５で作成され（Ｓ６）、暗号鍵共有部７で公開鍵暗号方式を用いて受信側に送信され、受信側と暗号鍵の共有を行う（Ｓ７）。この暗号鍵の共有が完了すると、データ暗号化部４において分割番号を含めた分割データを暗号鍵を用いて暗号化処理し（Ｓ８）、暗号化されたデータを順番にデータ送信部８から受信側に送信する（Ｓ９）。この時、暗号化処理とデータ送信は同時に動作する処理であり、ｎ個目の分割データが暗号化処理されている時にはｎ－１個目の暗号化データが送信される。暗号データの送信が完了すると終了メッセージを送信して通信を終了する（Ｓ１０）。

【００３１】受信側では、通信接続の際に暗号通信が通知（Ｓ２１：Ｙ）されると、受信側の暗号鍵が暗号鍵共有部９で共有され（Ｓ２２）、暗号化データの受信準備が完了する。

【００３２】暗号化データはデータ受信部１０によって受信され（Ｓ２３）、送信側と共有された６４個の暗号鍵を用いてデータ復号化部１２によって復号処理され（Ｓ２４）、データ蓄積部１３に蓄積される。蓄積されたデータは、列毎のデータ順に並べられているので、データ合成部１４では各蓄積データの１バイト目から順番に並び替えることによって全体のデータを合成する（Ｓ２５）。合成されたデータはデータ出力部１５によって出力され（Ｓ２６）、最終的に送信データ全体を出力することができる。通信終了メッセージを受信すると、通信を終了する（Ｓ２７）。

【００３３】このように、送信データをＮ行×Ｍ列のデータに分割し、各列毎にデータを合成してひとつの分割データとし、この分割データをそれぞれ異なる暗号鍵を用いて暗号化処理を行うことにより、より暗号強度の高い暗号通信を行うことが可能となる。

【００３４】

【発明の効果】以上説明したことから明かなように、本発明の請求項１に記載の暗号通信方式によれば、送信側では、送信データを特定の大きさに分割して、その分割されたデータに順番に番号を付けて蓄積する一方、前記番号が付けられた分割データをそれぞれ暗号鍵を用いて暗号化処理した後、その各暗号化データを前記分割回数分繰り返して受信側に送信し、前記受信側では、受信した前記各暗号化データを前記受信側と共有する前記暗号鍵を用いて復号処理し、その復号された各分割データを前記番号の順番に従って合成するようにしたので、データを分割した分割データを順次暗号化処理して送信することにより、高速に暗号化データの送信を行うことができる。

【００３５】また、請求項２に記載の暗号通信方式によれば、送信側では、送信データを特定の大きさに分割して、その分割されたデータに順番に番号を付けて蓄積する一方、前記分割数と同数の互いに異なる暗号鍵を生成して、それ等の暗号鍵と前記各分割データの番号とを１対１に対応させると共に、前記各分割データをそれぞれ対応する前記暗号鍵を用いて暗号化処理した後、その各暗号化データを前記分割回数分繰り返して受信側に送信し、前記受信側では、受信した前記各暗号化データを前記受信側と共有する前記各暗号鍵を用いて復号処理し、その復号された各分割データを前記番号の順番に従って合成するようにしたので、分割した分割データをそれぞれ異なる暗号鍵で暗号化することにより、データの機密性の高い暗号通信を行うことができる。

【００３６】さらに、請求項３に記載の暗号通信方式よれば、送信側では、送信データをｎバイト単位でＮ行×Ｍ列に分割して、その各列毎にの列方向のデータを合成することにより、Ｎ×ｎバイトのデータを作成して、各列のデータ毎にｉ（１≦ｉ≦Ｍ）の番号を付けて蓄積する一方、そのＭ列と同数の互いに異なる暗号鍵を生成して、それ等の暗号鍵と前記各分割データの番号とを１対１に対応させると共に、前記各分割データをそれぞれ対応する前記暗号鍵を用いて暗号化処理した後、その各暗号化データを前記Ｍ回分繰り返して受信側に送信し、前記受信側では、受信した前記各暗号化データを前記受信側と共有する前記各暗号鍵を用いて復号処理し、その復号された各分割データを前記Ｎ行×Ｍ列に合成するようにしたので、分割した分割データをそれぞれ異なる暗号鍵で暗号化することにより、データの機密性が一層高い暗号通信を行うことができる。

【図面の簡単な説明】

【図１】本発明の実施の形態における暗号通信方式の構成を示すブロック図である。

【図２】暗号通信方式の送信手順を示すフローチャートである。

【図３】暗号通信方式の受信手順を示すフローチャートである。

【図４】暗号通信方式の分割データのフォーマットを示す図である。

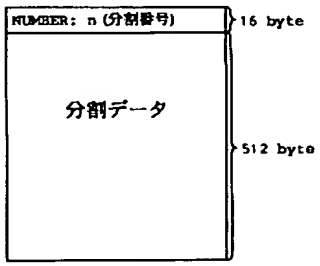
【図５】本発明の他の実施の形態における暗号通信方式のＮ行×Ｍ列の分解データのフォーマットを示す図である。

【図６】他の実施の形態における暗号通信方式の分割データのフォーマットを示す図である。

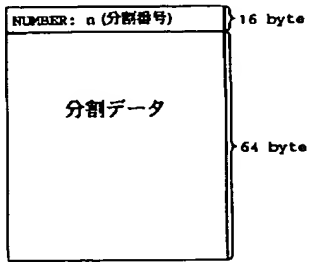
【符号の説明】

１　データ入力部
２　データ分割部
３　データ蓄積部
４　データ暗号化部
５　暗号鍵生成部
６　送信側制御部
７　暗号鍵共有部
８　データ送信部
９　暗号鍵共有部
１０　データ受信部
１１　受信側制御部
１２　データ復号化部
１３　データ蓄積部
１４　データ合成部
１５　データ出力部

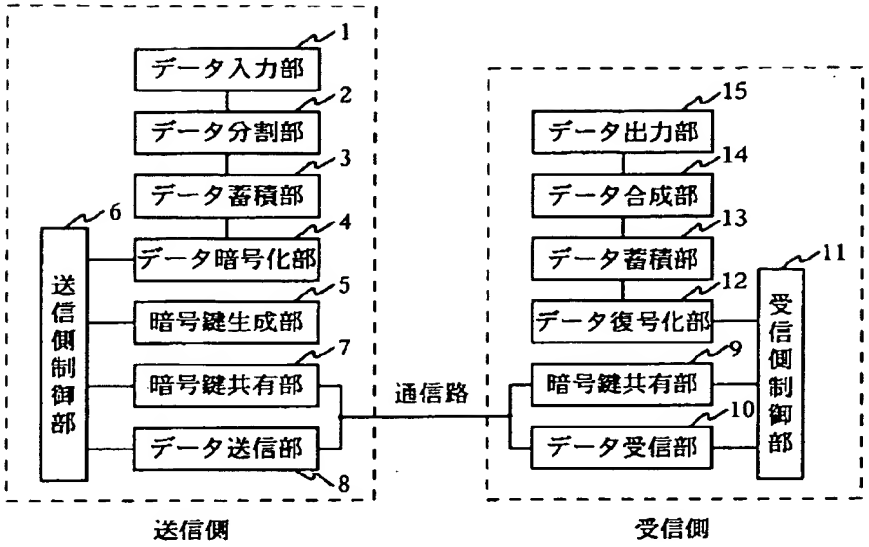
【図４】



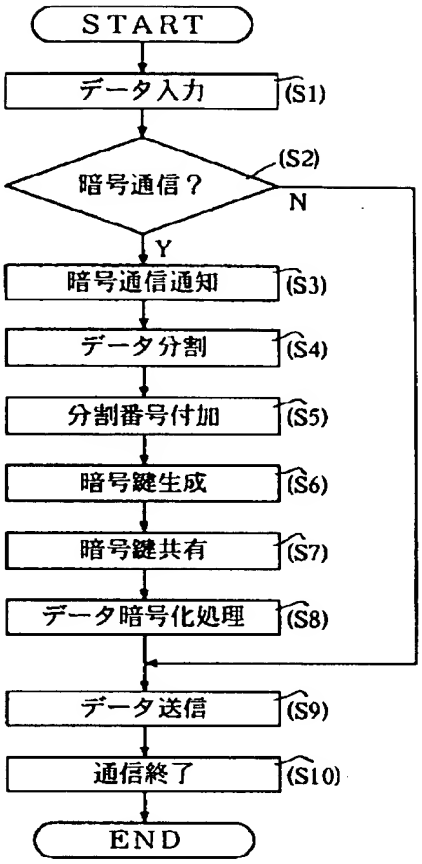
【図６】



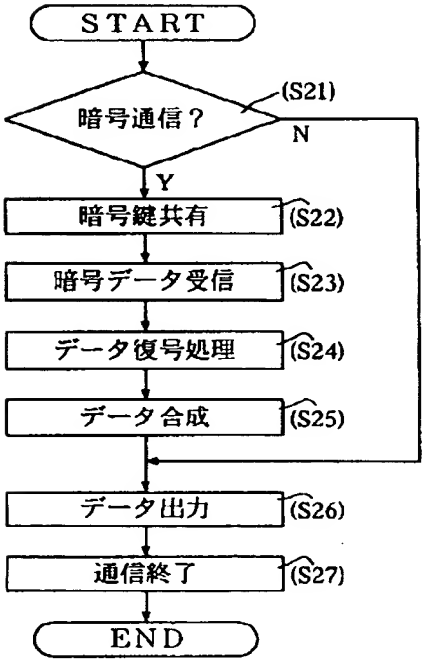
【図1】


1
データ入力部
2
データ分割部
3
データ蓄積部
6
送信側制御部
4
データ暗号化部
5
暗号鍵生成部
7
暗号鍵共有部
データ送信部
8
通信路
15
データ出力部
14
データ合成部
13
データ蓄積部
11
12
データ復号化部
9
暗号鍵共有部
10
データ受信部
受信側制御部
送信側
受信側

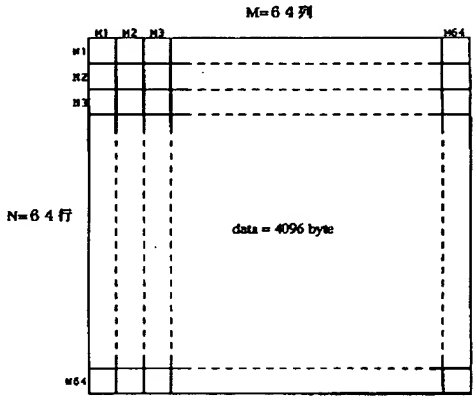
【図2】


START
データ入力
(S1)
暗号通信？
(S2)
N
Y
暗号通信通知
(S3)
データ分割
(S4)
分割番号付加
(S5)
暗号鍵生成
(S6)
暗号鍵共有
(S7)
データ暗号化処理
(S8)
データ送信
(S9)
通信終了
(S10)
END

【図3】


START
暗号通信？
(S21)
N
Y
暗号鍵共有
(S22)
暗号データ受信
(S23)
データ復号処理
(S24)
データ合成
(S25)
データ出力
(S26)
通信終了
(S27)
END

【図5】


M=64列
M1
M2
M3
M64
N=64行
data = 4096 byte